

REMARKS

Claims 1-35 are pending in the present application.

This Amendment is in response to the Office Action mailed July 2, 2007. In the Office Action, the Examiner rejected claims 1-32 under 35 U.S.C. § 102(e) and claims 33-35 under 35 U.S.C. § 103(a). Applicant has cancelled claims 2, 10, 18, 26 and amended claims 1, 9, 17 and 25. Reconsideration in light of the remarks made herein is respectfully requested.

I. REJECTIONS UNDER 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 1-32 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,677,888 issued to Roy ("Roy"). Applicant respectfully traverses the rejection for the following reasons.

Roy discloses a secure Aircraft Addressing and Reporting System (ACARS) solution for protecting the aeronautical information transfer end-to-end over the ACARS data link using standard-based, cryptographic techniques (Col. 3. lines 5-8). Roy discloses a solution to encrypt ACARS protocol header. It also defines protocol to derive secret keys. However, in contrast to the present invention, its secret key derivation is based on random number generated by ground SAM. In the present invention, the secret key derivation is based on using DSA type of digital certificate domain parameters (i.e., p_{dss} , q_{dss} , g_{dss}). By using the domain parameters, the exponential operations to generate shared secret key is only 3, while in Diffie-Hellman (DH) key exchange, 4 exponential operations is needed.

Roy discloses that on receipt of a request message, the ground SAM would obtain a certificate of the aircraft and the latest of CRL from a certificate depository (CD)... It then verifies the signature at s_u , using ECDSA algorithm (Col. 10, lines 58-

64). Roy also discloses that according to ECDSA signature and verification operations, to generate a key pair, an entity first selects an elliptic curve E and a point G on E . The entity then selects a private key d , which is an integer picked at random, and computes the public key dG . To sign a message M , the SAM processes M with a known hash function called SHA-1,... Then the entity selects an integer k at random, ... When the receiving SAM process wants to verify the signature (r,s) on the message M it retrieves the public key $Q=dG$ of the sending... The signature is genuine if the two values are equal (Col. 9, lines 41-60). The certificate authority (CA), which is a trusted entity that issues the asymmetric cryptographic keys, the public key certificates, and the Certificate Revocation Lists (CRL)... the domain parameters and the key size determine the cryptographic strength (Col. 10, lines 27-32). Roy discloses that to establish a secret session key, the airborne SAM creates an Initialization_request message. The airborne SAM signs this message and sends this message with the signature to the ground SAM. (Col. 10, lines 48-52). Roy also discloses the elliptic curve Diffie-Hellman (DH) key agreement scheme operation that shown in Col. 10 (lines 1-9).

Regarding Col. 10, lines 58-64 of Roy, applicant is well aware that the certificate obtained from the aircraft can be considered as the first certificate, as well as, the first certificate can be obtained from any protocol. The certificate can be part of any network protocol, for example, IKE (Internet Key Exchange) protocol, or SSL (Secured Socket Layer) protocol... Also, applicant is also aware that all protocols exchange certificates during a hand shake and that certificate is digitally signed. However, the present invention is not about issuing a certificate as disclosed in Roy but to utilize parameters from a certificate to generate a secret key by using only 3 exponential operations.

Regarding Col. 9, lines 41-60 of Roy, these lines talk about generating ECC certificate. Unlike Roy, in the present invention, that certificate is assumed to have been issued by CA already. Each peer just uses DSA parameters from already issued certificates. This operation calculates only new public/private key by using DSA parameters from the certificate. Then the new generated public key is sent to the first peer, along with the second peer certificate where part of protocol for session key derivation is disclosed in paragraphs 39 to 40.

Regarding Col. 10, lines 27-32 of Roy, it is true that each system can choose to use some CA and that key sizes can be defined as well. However, the present invention is not about defining and enrolling certificates. The operations in the present invention assume that certificates are already issued by CA and both peers have DSA type of certificates and that they are valid.

Regarding Col. 10, lines 48-52 of Roy, these lines describe protocol between an aircraft and ground SAM. The present invention does not claim protocol but a key exchange method or a key establishment method, which can be used in any protocol (including those protocols disclosed in Roy).

Regarding Col. 10, lines 1-9 of Roy, these lines discuss how Diffie-Helman (DH) shared secret key is established on ECC. In contrast to the present invention, where DSA parameters are used; these DSA parameters are not the same as DH parameters. Furthermore, the first peer does not generate DH public/private key but it just sends a certificate. The second peer generates one time public/private key pair by using domain parameters (i.e., DSA parameters), which are not the same as DH parameters. In summary, classic DH key exchange requires 4 exponentiation operations (2 operations on each side): one for generating DH public/private key and

one for generating shared secret key on each side. The claimed invention generates the shared secret key by 3 exponentiation operations only by using DSA parameters.

To support a 102 rejection, the Examiner must show that “each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” Verdegaal Bro. v. Union Oil Co. of California, 814 F.2d 628, 631 (Fed. Cir. 1987), (MPEP §2131). In addition, “[t]he identical invention must be shown in as complete detail as is contained in the ... claim.” Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989), (MPEP §2131). Here the Examiner has not pointed out the specific language in Roy that teaches generating a secret key by 3 exponential operations using DSA parameters.

Roy does not disclose, suggest, nor render obvious generating a secret key by 3 exponentiation operations using DSA parameters. In other words, no where in Roy that discloses using DSA parameters to generate a secret key by only 3 exponential operations.

Since the Examiner has failed to show the identical invention in as complete detail as is contained in the claim, the rejection under 35 U.S.C. §102(b) was improperly made. Therefore, Applicant respectfully requests that rejection be withdrawn.

II. REJECTIONS UNDER 35 U.S.C. § 103

The Examiner rejected claims 33-35 under 35 U.S.C. § 103(a) as being unpatentable over Roy and further in view of U.S. Patent No. 7,222,187 issued to

Yeager ("Yeager"). Applicant respectfully traverses the rejection for the following reasons.

Yeager discloses that in order to interact with other peers; the peer needs to be connected to some kind of network, such as IP, Bluetooth, or Havi, among others (Col. 27, lines 29-35). Yeager further discloses that the peer-to-peer platform may be independent of transport protocols. For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, Home-PNA, and other protocols (Col. 33, lines 21-25). Yeager, however, does not disclose generating a secret key by 3 exponentiation operations using DSA parameters.

Roy, Yeager, taken alone or in any combination, do not disclose, suggest, nor render obvious generating a secret key by 3 exponentiation operations using DSA parameters. This aspect of the invention is supported in the specification on paragraphs 7-8, 39-43 and is recited in amended claims 1, 9, 17 and 25.

Therefore, Applicant believes that independent claims 1, 9, 17, 25 and their respective dependent claims are distinguishable over the cited prior art references. Accordingly, Applicant respectfully requests the rejections under 35 U.S.C. § 102(b) and § 103(a) be withdrawn.

CONCLUSION

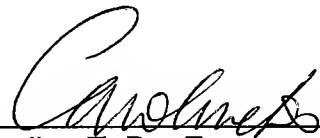
In view of the amendments and remarks made above, it is respectfully submitted that the pending claims are in condition for allowance, and such action is respectfully solicited. If it is believed that a telephone conversation would expedite the prosecution of the present application, or clarify matters with regard to its allowance, the Examiner is invited to contact the undersigned attorney at the number listed below.

The Commissioner is hereby authorized to charge payment of any required fees associated with this Communication or credit any overpayment to Deposit Account No. 04-1175.

Respectfully submitted,

DISCOVISION ASSOCIATES

Dated: 08/24/07



Caroline T. Do, Esq.
Reg. No. 47,529

DISCOVISION ASSOCIATES
INTELLECTUAL PROPERTY DEVELOPMENT
2265 E. 220th Street
Long Beach, CA 90810
(310) 952-3300